UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,265	12/28/2001	Koichi Ito	1573.1010	2775

21171   7590   09/01/2006

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
SZYMANSKI, THOMAS M

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *14 August 2006*.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *4,8,9,32-41,50-57 and 64-72* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *4,8,9,32-41,50-57 and 64-72* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on *12/28/2001* is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 4, 8-9, 32-41, 50-57, and 64-72 have been examined.

2.   The Final Rejection of 5/16/2006 has been withdrawn.

Specification

3.   Applicant is reminded of the proper language and format for an abstract of the

disclosure.

The abstract should be in narrative form and generally limited to a single

paragraph on a separate sheet within the range of 50 to 150 words. It is important that

the abstract not exceed 150 words in length since the space provided for the abstract

on the computer tape used by the printer is limited. The form and legal phraseology

often used in patent claims, such as **"means"** and "said," should be avoided. The

abstract should describe the disclosure sufficiently to assist readers in deciding whether

there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information

given in the title. It should avoid using phrases which can be implied, such as, "The

disclosure concerns," "The disclosure defined by this invention," "The disclosure

describes," etc. The abstract as currently provided contains the language "means" on

lines 4, 8, and 10.

4.   The specification is objected to as failing to provide proper antecedent basis for

the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction

of the following is required: The terms $S[x]$, $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$, and $S_j[x]$ are not

clearly defined, the claims attempt to indicate this as being an i-th masked fixed table

but the specification denotes on page 25 lines 28-30 that it is an ith fixed S-box, whereas $FM_{i,h}$, $FM_{in,h}$ and $FMout_h$ are fixed mask values according to tables of q order where q is at least 3 or more, as presently understood.

Drawings

5.   New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because Fig 28 defines the output of the Sbox as Y, which corresponds to $S_j[Y]$, however as currently indicated in the drawing it is being reciprocally redefined as $S_j[x\ XOR\ c_{i,j}]\ XOR\ d_{i,j}$, and $S_j[x]$, which makes the recitation indefinite since it is not clear to which x reference is being made. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Objections

6.   Claims 4, 8, 34, and 37 objected to because of the following informalities: The stated claims do not contain periods at the end of the claim recitation or contain a double period as in the case of claim 4. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8.   Claims 4, 8-9, 32-41, 50-57, and 64-72 rejected under 35 U.S.C. 112, second

paragraph, as being indefinite for failing to particularly point out and distinctly claim the

subject matter which applicant regards as the invention.

9.   Claims 4 recites "q sets of fixed values" in line 5 and 8 to refer to different data. It

is not clear exactly which sets of values q is defining from this recitation. The recitation

from claim 50, which states: "q sets of masked fixed values and q sets of fixed tables,

where q is an integer equal to three or more,.." appears to better express this

relationship. However the selection of the corresponding value in relation to the random

number h is not clear, since the claims provide no mapping of the relation between the

masks such as $FM_{i,h}$ and $FM_{i,q-1}$.

10.   Additionally, the claims provide for no clear indication of what the values of $FM_{i,h}$

indicate regarding if they are fixed tables or mask values in a fixed table form.

11.   Claim 4 further recites "a fixed table before masking is defined as S[x], and i-th

masked fixed table is defined as $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$ for the j-th fixed value", this

appears to be defining the operation of creating an S-box as outlined on page 26 and

Fig 28 of the applicant's disclosure and further renders the definition indefinite for using

x to define two separate values with respect to $S_j[x]$, wherein it appears that it should be

denoted as $S_j[Y]$.

12.   Claim 4 further denotes a value C_h and D_h, but provide no requisite for

ascertaining what these values indicate and how they comprise satisfying the stated

equations.

13.   Claim 4 recites the limitation "j is an integer" in line 7. There is insufficient antecedent basis for this limitation in the claim.

14.   Claim 8 recites "$FM_{0,h} = C_h$ XOR $L1_0(FMin)$, $C_h = C_{h,15} C_{h,1} .... C_{h,0}$, and $D_h = d_{h,15} d_{h14} ... d_{h,0}$ are satisfied, where $FM_{i,h}$ is the i-th...." The terms "$FM_{0,h}$" and "$FM_{i,h}$" as defining the same thing but occur as a static value 0 and a round dependent value i making the definition indefinite. Additionally, $L1_0$ is defined in relation to "$FM_{0,h}$" as a single round transformation when clearly the indication is toward the overall process. "FMin" has not been defined and has no antecedent basis in the claim, such a recitation is believed to intend "$FMin_{i,h}$", which represents a separate fixed table of mask values. Additionally, as stated above in relation to satisfying the equation no conditions have been listed for satisfying the equation, but it appears merely as a definition. Lastly, no "D_h" is present within the stated equation making it unclear how such a condition is to be satisfied with the stated variable.

15.   Claims 9, 32, 33, 34, 35, 39, 40, 41, 51, 52, 53, 55, 56, 57, 65, 66, 67, 69, 70, 71, contain contradictory definitions of the claimed transform means. The first transform means has been attempted to both be defined as a shift and a simple linear relation, and the second linear transform has been both defined as a mixed columning and a shift operation. Specifically see claims 9, and 32-34.

16.   The above issues as related to claims 4 and 8 are meant as exemplary issues which occur through the subsequent independent claims.

Claim Rejections - 35 USC § 102

17.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

18.   Claims 4, 8-9, 32-41, 50-57, and 64-72 are rejected under 35 U.S.C. 102(b) as

being anticipated by Kawamura et al European Patent Application EP 0981223 A2.

19.   Regarding Claims 4, 38, 54, 68: An encryption device comprising XOR means

and nonlinear transform means, said encryption device further comprising:

a random number generator for generating a random number h, where h is an

integer between zero and q-1; (paragraph 9, 43-45, Fig 4) as noted "means for

randomly selecting one pattern of each of pairs....", whereby from the figure it is clear

such an indication begins at 0 and as noted would necessitate i-1, which is equivalent to

q-1.

q sets of fixed values, where q is an integer equal to three or more (paragraphs

9-13, Fig 4) As noted in the prior art there may be any number of sets of masks greater

than 1, where the sets are denoted ai where i is a positive integer not less than one,

anticipating 3 or more.

wherein equations, $FM_{i,h} = C_h$ XOR $L1i(L2i-1(Dh))$ for $i \geq 1$, $C_h = C_{h,15} C_{h,1}....C_{h,0}$,

and $D_h = dh_{,15}dh_{14}...d_{h,0}$, where i is an integer and j is an integer, q sets of fixed values,

wherein equations, $(c_{0,j}$ XOR $c_{1,j}) = (0101...01)_2$ or $(1010...10)_2$ and $(d_{0,j}$ XOR $d_{1,j}) =$

$(0101...01)_2$ or $(1010...10)_2$ are satisfied, (Fig 4, paragraphs 33-37, 47-52) The

hamming weights discussed anticipate these conditions.

a fixed table before masking is defined as $S[x]$, and i-th masked fixed table is

defined as $S_j[x\ XOR\ c_{i,j}]\ XOR\ d_{i,j}$ for the j-th fixed value; (Fig 2, 4, 15, paragraphs 39-41,

78-80) As stated the S-box is xor'ed with the mask values.

linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the

linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed

table $S_j[x]$ and the linear transform means $L2_i(x)$ operate in i-th one of rounds; and (Fig

13-14, paragraphs 67-75) The process of DES denotes the use of 2 linear

transformations and the s-box which is non-linear.

a first selector for selecting one fixed value of the h-th set of said q sets of fixed

values of said q sets of fixed tables in response to the random number h,

said XOR means XORing an input thereto with an XOR of a key with said selected fixed

value. (Fig 4, 16-17, paragraphs 43-45, 81-90) see figures and associated discussion.

20.   Regarding Claims 8, 50, 64, 72: q sets of fixed values, where q is an integer

equal to three or more, wherein equations, $FM_{o,h} = C_h\ XOR\ L1_0(FMin)$, $C_h = C_{h,15}$

$C_{h,1}....C_{h,0}$, and $D_h = dh_{,15}dh_{14}...d_{h,0}$ are satisfied, where $FM_{i,h}$ is the i-th fixed value of the

h-th set of said q sets of fixed values, where i is an integer and j is an integer,

q sets of fixed values, wherein equations, $(c_{0,j}\ XOR\ c_{1,j})\ v\ (c_{1,j}\ XOR\ c_{2,j})\ v...v\ (c_{q-2,j}$

$XOR\ c_{q-1,j}) = (111\ ...\ 11)_2$ and $(d_{0,j}\ XOR\ d_{1,j})\ v\ (d_{1,j}\ XOR\ d_{2,j})\ v...v\ (d_{q-2,j}\ XOR\ d_{q-1,j}) = (111$

$...\ 11)_2$ are satisfied, (Fig 4, paragraphs 33-37, 47-52) As noted above the hamming

weights indicate such relations.

21.   Regarding Claims 9, 32-35, 39-41, 51-53, 55-57, 65-67, and 69-71 linear transform means $L1_i(x)$ comprises means for shifting an input, $L2_i(x)$ comprises means for mixed columning an input, $L2_i(x)=MixedColumn(Shift(x))$, $L2_i(x)=shift(x)$, $L1_i(x)=x$. (Fig 4, 13-14, paragraphs 67-75) The process of DES denotes the use of 2 linear transformations (shift and mixed columning) and the s-box which is non-linear.

22.   Claims 32-41, 50-57, and 64-72 are rejected on the same grounds as claims 4, 8, and 9 as noted above. Claims 32-41, 50-57, and 64-72 containing the same subject matter as the above rejected claims.

Conclusion

23.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Szymanski whose telephone number is 571-272-8574. The examiner can normally be reached on M-F 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571-272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TMS
8/28/2006

JACQUES LOUIS JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100